UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/691,278	10/17/2000	Radia J. Perlman	SUN-P5343-RSH	4965

57960 7590 06/02/2006

SUN MICROSYSTEMS INC.
C/O PARK, VAUGHAN & FLEMING LLP
2820 FIFTH STREET
DAVIS, CA 95616

EXAMINER	
CALLAHAN, PAUL E	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 06/02/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/691,278	PERLMAN	
	Examiner	Art Unit	
	Paul Callahan	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 March 2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-11,13-29,31-47 and 49-54* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☐ Claim(s) *1-11, 13-29, 31-47, and 49-54* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-11, 13-29, 31-47, and 49-54 are pending and have been examined.

Response to Arguments

2. Applicant's arguments filed 3-17-06 have been fully considered but they are not persuasive.

The applicant argues in traverse of the rejections of the claims as found in the previous Office Action in the case by asserting that the instant invention may be distinguished from the teachings of the applied prior art by virtue of the instant claims teaching the use of a temporary secret key that is distinguishable from the secret key taught by Medvinski et al in the generation of a ticket. The applicant argues that such a key, with a limited lifespan intended to decrease the vulnerability of the KDC is not taught by Medvinski. The applicant argues that both Medvinski and Kohl teach away from the instant invention:

As per the teachings of Kohl and Medvinski, the applicant argues that Keberos uses a long-term secret key, with a long lifetime, that is shared between a Key Distribution Center (KDC) and a server. Yet the establishment of a temporary secret key was taught by the Schneier Reference, with the temporary nature of the key being taught by Schneier in the cited section on page 47, Sec. 3.1 "Key Exchange", where it is taught that a temporary, session key is used for only one communications session. Schneier states: "...session keys are useful because they exist for only the duration of

the communication session." This does read on the applicant's temporary secret key, as do the cited portions of Medvinski and Kohl used in the rejection.

The applicant argues that a session key may be distinguished from the secret key of the instant invention based upon the purpose for which each is generated. The applicant argues that a session key is generated and exists for only the duration of one communication session, whereas the applicant's secret key has a defined lifespan. The Examiner points out that the language of a secret key having such a "defined" lifespan is not found in the claims. The claims are instead directed towards such a key having a "limited" lifespan, i.e., it will not exist indefinitely. A session key such as that taught by Schneier, one that exists for only the duration of one communications session, does indeed read on a key with a limited lifespan. In addition, Medvinski and Kohl do teach the use of key expiration times as noted in the rejection of the claims found in the previous Office Action.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1, 4, 5, 8, 9, 13, 15, 16, 18, 19, 22, 23, 26, 27, 31, 33, 34, 36, 37, 40, 41, 44, 45, 49, 51, 52, and 54 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Bruce Schneier, Applied Cryptography 2nd Edition, Oct. 1995, John Wiley & Sons Pub. Pages 43-57, in view of Medvinski et al., "Public Key Utilizing Tickets For Application Servers" Internet Draft: Common Authentication Technology Working Group, March 1998, pages 1-6, and Kohl et al., "The Kerberos Network Authentication Service", Network Working Group Request For Comments (RFC) 1510, Sept. 1993.

As for claims, 1, 19, and 37; The claims each recite a method, a computer program-product causing a system to carry out a method, and a system configured to carry out the method, where a communication from a server is received at a key distribution center, where the communication is authenticated, and where the communication contains a secret key which is then stored at the key distribution center.

Schneier teaches a method by which a key may be sent from one communicant to another by means of an authenticated communication in Chapter 3: "Basic Protocols" pages 47-57, where a session key is distributed from one communicant to another via a public key protocol. The message is taught as authenticated by virtue of its decryption by a receiver using a public key of a sender, the sender passing a message and key encrypted under a private key held only by the sender and uniquely corresponding to the sender's public key. Schneier teaches the use of such distribution of session keys by public key techniques involving key distribution centers and servers in pages 43-44: "Attacks Against Public Key Cryptography." Schneier does not teach the additional limitation of a temporary secret key being encrypted with a public key belonging to the KDC, so that the temporary secret key can only be decrypted using a private key

belonging to the KDC. However. Medvinski et al. teach this feature in a public key extension to the Kerberos protocol (page 2, PKTGS_REQ: Client to Server). Medvinski teaches the use of a secret key with a limited lifespan intended to reduce KDC vulnerability (page 57: "Key Expiration"). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this feature of Medvinski into the system of Schneier. Motive to make the combination is found on page 1 of Medvinski Sec. 2; "Introduction" where the advantage of Public Key extensions to Kerberos is discussed.

Schneier teaches a new, temporary, secret key is that is subsequently generated to replace an invalid temporary secret key (page 47, Sec. 3.1: "Key Exchange": where a secret or session key is valid for only one communication session, and a new one is generated for each new session).

The combination of Schneier and Medvinski does teach a temporary secret key that becomes invalid after a specified time (Medvinski, page 57 "Key Expiration"). However Kohl teaches this feature as well, and somewhat more explicitly (Section 3.1.5, final paragraph, Section 3.3.3 final paragraph). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate these features into the system of Schneier and Medvinski. It would have been desirable to do so as this would decrease the likelihood of replay attacks using an old key.

As for claims 4, 22, and 40, Medvinski teaches the feature of the claim that Schneier does not, namely wherein assembling the message involves including an

expiration time for the session key in the message (page 2, sec. 3, PKDA Background: Timestamp). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this feature of Medvinski into the system of Schneier. It would have been desirable to do so as the use of a timestamp and expiration date for the key would prevent a replay attack by an eavesdropper.

As for claims 5, 23, and 41, Schneier teaches a step where allowing the client to forward the ticket to the server includes allowing the client to forward an identifier for the temporary secret key to the server so that the server can know which temporary secret key to use in decrypting the ticket (page 568, Credentials, where the client i.d. is authenticated and serves as a session key identifier).

As for claims 8, 26, and 44, Schneier teaches the step of receiving the communication from the server involves authenticating the server (page 570, "Requesting a Service").

As for claims 9, 27, and 45, Schneier teaches a step of authenticating the server that involves using authentication information pertaining to the server, the authentication information including a certificate chain from a trust anchor to the server, and including a server public key that is associated with a server private key to form a public key-private key pair associated with the server (page 575-577: "Certificates").

As for claims 13, 31, and 49, Schneier teaches a step wherein the communication is signed with a server private key so that the KDC can use a corresponding server public key to verify that the communication was sent by the server (page 53-54: "Authentication Using Public Key Cryptography).

As for claims 15, 33, and 51, Schneier teaches communicating information to the server that enables the server to authenticate the KDC (pages 53-54, Authentication Using Public Key Cryptography).

As for claims 16, 34, and 52, Schneier teaches a KDC operating in accordance with the Kerberos standard (page 60, Kerberos).

As for claims 18, 36, and 54, Medvinski teaches the features of the claim not taught by Schneier, namely propagating the temporary secret key to multiple KDCs (page 5, sec. 5.1.3. "Cross realm Authentication"). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this feature into the system of Schneier. It would have been desirable to do so as this would allow for distributed authentication across many domains.

5. Claims 14, 17, 32, 35, 50, and 53 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bruce Schneier, Applied Cryptography 2nd Edition, Oct. 1995, John Wiley & Sons Pub. Pages 43-57, in view of Medvinski et al., "Public Key Utilizing Tickets

For Application Servers" Internet Draft: Common Authentication Technology Working Group, March 1998, pages 1-6, and Official Notice taken as detailed below.

As for claims 14, 32, and 50, Official Notice may be taken that the step of an initial key request message sent by a KDC to the server indicating that the temporary secret key is needed from the server is old and well known in the art of secure communications. A good example of this process is one found in the registration of new nodes in multicast systems. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this feature into the system of Schneier and Medvinski. It would have been desirable to do so as this would allow for rapid client-server service request response processing.

As for claim 17, 35, and 53, Official Notice may be taken that the step of an authentication communication received from a server that additionally includes an identifier for the server is one that is old and well known in the art of secure communications. Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this feature into the system of Schneier and Medvinski. It would have been desirable to do so as such an identifier would allow for mutual authentication of the server and KDC.

6. Claims, 2, 3, 6, 7, 10, 11, 20, 21, 24, 25, 28, 29, 38, 39, 42, 43, 46, and 47 are rejected under 35 U.S.C. 103(a) as being unpatentable over Bruce Schneier, Applied

Cryptography 2nd Edition, Oct. 1995, John Wiley & Sons Pub. Pages 43-57, in view of Medvinski et al., "Public Key Utilizing Tickets For Application Servers" Internet Draft: Common Authentication Technology Working Group, March 1998, pages 1-6, Sirbu et al., "Public Key Based Ticket Granting Service in Kerberos" Internet-Draft, May 6, 1996, pages 1-16, and Official Notice taken as detailed below.

As for claims 2, 20, and 38, Sirbu and Chuang teach the limitations of these claims that the combination of Schneier and Medvinski et al. fails to teach, namely where upon receiving a request from a client at the KDC to communicate with a server, further facilitating communications between the client and the server by: producing a session key to be used in communications between the client and server; (page 2, Sec. 3.1 PK Kerberos Operation) creating a ticket to the server by encrypting an identifier for the client and the session key with the temporary secret key for the server (page 3, Sec. 3.1: PK Kerberos Operation); and assembling a message that includes the identifier for the server, the session key and the ticket to the server; and sending the message to the client in a secure manner (page 3, Sec. 4: Message Exchanges); and allowing the client to forward the ticket to the server in order to initiate communications between the client and the server (page 3, Sec. 4: Message Exchanges). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this feature of Sirbu et al. into the system of Schneier and Chuang. Motive to make this combination is found for example in page 2 sec. 2 of Sirbu et al., where the absence of long term storage of secret keys is discussed.

As for claims 3, 21, and 39, Sirbu and Chuang teach the features of the claim not taught by the combination of Schneier and Medvinski, namely, upon receiving the ticket from the client at the server, the method further comprises: decrypting the ticket at the server using the temporary secret key to restore the session key and the identifier for the client (pages 2-3, Sec. 3.1 PK Kerberos Operation, page. 5, Sec. 4.2.2: Receipt of PKTGS-ReQ); and using the session key at the server to protect subsequent communications between the server and the client. (pages 2-3, Sec. 3.1 PK Kerberos Opération, page. 5, Sec. 4.2.2: Receipt of PKTGS-ReQ). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this feature of Sirbu et al. into the system of Schneier and Chuang. Motive to make this combination is found for example in page 2 sec. 2, where the absence of long-term storage of secret keys is discussed.

As for claims 6, 24, and 42, Sirbu et al. teach the features of the claims that the combination of Schneier and Medvinski do not teach, namely wherein sending the message to the client in the secure manner involves encrypting the message with a second session key that was previously communicated to the client by the KDC (page 2 sec. 3.1 PK Kerberos Operation). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this feature into the system of Schneier and Medvinski. It would have been desirable to do so as this would allow for reduced computational overhead in the message exchange.

As for claims 7, 25, and 43, Sirbu et al teaches the features of the claim not taught by the combination of Schneier and Medvinski, namely alternatively creating the ticket to the server by encrypting the identifier for the client and the session key with one of: a public key for the server; and a secret key for the server previously agreed upon between the server and the KDC and stored at the KDC (page 7 Sec. 5.3 PKTGS-REQ). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this feature into the system of Schneier and Medvinski. It would have been desirable to do so as this would allow only an entity knowing the secret key associated with the public key of the server to decrypt.

As for claims 10, 28, and 46, Sirbu et al. teach a step wherein authenticating the server involves authenticating the server without having prior configuration information pertaining to the server at the KDC (page 2 sec. 1 Motivation). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this feature into the system of Schneier and Medvinski. It would have been desirable to do so as this would allow for authentication directly between a client and server without the computational overhead associated with a trusted third party.

As for claims 11, 29, and 47, Sirbu teaches the features of the claim not taught by the combination of Schneier and Medvinski, namely authenticating the server includes using a server public key that is stored locally in the KDC (page 2 sec. 3.1 PK

Kerberos Operation). Therefore it would have been obvious to one of ordinary skill in the art at the time of the invention to incorporate this feature into the system of Schneier and Medvinski. Motive to make the combination is found on page 1 of Medvinski Sec. 2; "Introduction" where the advantage of Public Key extensions to Kerberos is discussed.

Conclusion

7. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Paul E. Callahan whose telephone number is (571) 272-3869. The examiner can normally be reached on M-F from 9 to 5.

If attempts to reach the examiner by telephone are unsuccessful, the Examiner's supervisor, Emmanuel Moise, can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is: (571) 273-8300..

5-26-06

Paul Callahan

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER